REMARKS

Reconsideration is requested in view of the preceding amendments and the following remarks. Claims 1, 2, 5, 12, 23, and 30 are amended, and new claims 39-43 are submitted for consideration. Support for new claims 39-43 can be found in the specification at, for example, page 6, line 6 to page 7, line 23. No new matter is introduced.

Claims 6, 15-22, and 31 have been previously cancelled, and any rejections of these claims are moot in view of their cancellation. The cancellation of these or any other claims is not an admission that any cancelled claim or feature in a cancelled claim is unpatentable.

Applicant regrets that claims 27 and 37 were erroneously referred to in the preceding Amendment. As presently understood, the Office action contends that claim 5 had not been amended to include a stop condition that is an expiration time of a request. Claim 5 was amended to include this feature, and clarification is requested.

In so far as any rejections in the Office action are based on contentions that certain features are well known but are stated without a proper citation of references, applicant requests that references be provided for all such contentions.

Rejections under 35 U.S.C. § 112

Claims 5 and 12 stand rejected under 35 U.S.C. § 112, second paragraph, as failing to set forth the subject matter which the applicant regards as his invention. This rejection is traversed. These claims have been amended for clarification. Regardless of any amendment to these claims, withdrawal of this rejection is requested. The Office action contends that the invention "is different from what is defined in the claim(s) because the original specification and the

original claims merely disclose monitoring a stop condition indicating when to stop or terminate intrusion detection services wherein the stop condition is an expiration time." Office action, page 4. This rejection is improper and should be withdrawn. According to the MPEP,

> The content of applicant's specification is not used as evidence that the scope of the claims is inconsistent with the subject matter which applicants regard as their invention. As noted in *In re Ehrreich*, 590 F.2d 902, 200 USPQ 504 (CCPA 1979), agreement, or lack thereof, between the claims and the specification is . . . irrelevant to compliance with the [35 U.S.C. § 112] second paragraph. MPEP § 2172.

The Office action explicitly uses the contents of applicant's specification in making this rejection as is expressly forbidden. For at least this reason, withdrawal of this rejection is requested.

Rejections in View of Yavatkar

Claims 1-4, 7-11, 13-17, 19-25, 27-36, and 38 stand rejected under 35 U.S.C. § 102(a) as allegedly anticipated by Yavatkar et al., "The Phoenix Framework: A Practical Architecture for Programmable Networks," IEEE Communications, pp. 160-165 (March 2000) (hereinafter "Yavatkar"). This rejection is traversed. (As noted above, any rejections of claims 15-22 and 31 are moot).

Amended claim 1 recites a method that comprises, in part, receiving a request from a central server at a software agent program to initiate intrusion detection services on a plurality of remote computers, wherein the request is issued in response to a notification of a network intrusion. Yavatkar does not teach or suggest such a method. The Office action cites Yavatkar as follows:

> We describe in this article Intel's framework for programmable networks. The objective of the Phoenix framework is to make it easier to deploy new network services that leverage the emerging trend toward use of reprogrammable network processors.

> The Phoenix framework defines a mobile agent system that allows an agent to be launched into the network to visit active devices and manipulate proactive services . . . the network administrators use the proactive consoles to install a new proactive service on active devices. Office action at page 1.

Applicant requests clarification. None of these cited portions of Yavatkar teaches or suggests installing intrusion detection services on a plurality of remote computers, *wherein the request is issued in response to a notification of a network intrusion* as recited in claim 1. Indeed, none of these portions even mentions intrusion detection. In order to anticipate a claim, a single reference must teach all claim features. This is plainly not so here, and claim 1 is allowable over Yavatkar.

The Office action further cites Yavatkar at page 165, first column and page 163, second column, in the rejection of claim 1. These portions of Yavatkar also fail to teach all the features of claim 1. Yavatkar's page 165, first column (see also Yavatkar, page 164, second column) discloses how a network administrator can trace the source of a TCP SYN attack using a watchdog agent and a bloodhound agent. According to Yavatkar, if the watchdog agent is unable to establish a connection with a server, the watchdog agent raises an alert and launches a bloodhound agent. The bloodhound agent is configured with the address of the server being attacked and is sent to the active device topologically closest to the attacked server. The bloodhound agent then finds the attack ingress point. These portions of Yavatkar do not teach or suggest "receiving a request from a central server at a software agent program to initiate intrusion detection services on a plurality of remote computers, wherein the request is issued by the central server in response to a notification of a network intrusion" as recited in claim 1. Instead, according to Yavatkar, intrusion detection services should be initiated on a single computer—the one closest to a point of attack. Yavatkar's page 163 contains a description of a

prototype system based on the Phoenix framework but does not mention intrusion detection at all. Applicant requests clarification. Because the cited portions of Yavatkar fail to teach all the features of claim 1, claim 1 and dependent claims 2-5, 7-14, and 39-43 are properly allowable over Yavatkar.

Claim 23 recites a method that comprises, in part, an intrusion detection server [that] is configured to send a request to install and execute intrusion detection software to software agents at a plurality of the computers based on at least one rule stored in a database. Yavatkar does not teach or suggest such a method. Yavatkar merely teaches sending a bloodhound agent to a network location nearest an attack. For at least this reason, claim 23 and dependent claims 24-29 are properly allowable.

Claim 30 recites an article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to perform network intrusion detection. The steps comprise receiving notification of a network intrusion; transmitting an installation request in response to the notification; and installing intrusion detection software on a plurality of remote computers via a software agent program in response to the request. In contrast, Yavatkar merely teaches sending a bloodhound agent to a network location nearest an attack, and not installing intrusion detection services on a plurality of remote computers. For at least this reason, claim 30 and dependent claims 32-38 are properly allowable over Yavatkar.

Rejections in View of Yavatkar and Porras

Claims 5, 12, 26, and 37 stand rejected as obvious in view of a combination of Yavatkar and Porras et al., U.S. Patent 6,484,203 ("Porras"). This rejection is traversed. Claims 5, 12, 26,

and 37 are properly allowable as dependent on allowable independent claims 1, 23, and 30. However, as described below, Yavatkar and Porras fail to teach or suggest the additional features of these dependent claims.

Amended claim 5 recites a method that includes, in part, monitoring for fulfillment of a stop condition, wherein the stop condition is an expiration time. The Office action fails to identify any portion of Yavatkar or Porras that teaches or suggest such a method. The cited portions of Porras concern monitoring suspicious network activity (col. 1, line 50 to col. 2, line 21), enterprise monitors that can focus on network-wide attacks (col. 3, lines 55-66), a response method that is initiated based on a response metric (col. 1, lines 15-31), detection of abnormal data transfers during workdays and weekends (col. 12, lines 23-40), and monitoring network health by detection of abnormal data loss based on historical norms that are a function of time of day (col. 5, lines 21-45). None of these portions of Porras mentions an expiration time for intrusion detection services.

The Office action contends that "Yavatkar discloses instantiate start and stop process of intrusion detection services which implicitly includes time to start and stop." While the inherent disclosure of a reference can be used in a rejection, the inherent feature must necessarily be present in the reference. Mere possibility that the reference could include the feature is not sufficient. See, for example, MPEP § 2112 at page 2100-47. Yavatkar does not mention an expiration time, and stopping of instruction detection services in Yavatkar could be based merely on having located the intrusion so that intrusion detection is no longer necessary. Thus, Yavatkar does not necessarily include an expiration time for intrusion detection services.

A *prima facie* case of obviousness requires that "the prior art references teach or suggest all claim features." MPEP § 2143. The Yavatkar/Porras combination does not teach or suggest

all the features of claim 5, and a *prima facie* case of obviousness has not been established. For at least this reason, claim 5 is properly allowable.

Amended claim 12 recites, in part, an expiration time for intrusion detection services. As noted above, the Yavatkar/Porras combination fails to teach this at least this feature of claim 12, and a *prima facie* case of obviousness has not been established. Accordingly, claim 12 is properly allowable.

Claim 26 recites changing a number of the plurality of computers executing intrusion detection software depending on time of day. The Yavatkar/Porras combination does not teach or suggest this feature. Porras teaches that network traffic is a function of time of day, and that abnormalities in network traffic should be detected based on time of day. The Office action contends that based on Porras, one of ordinary skill in the art would be motivated to provide more network resources based on time of day. Even if this contention were true, it is not what is claimed – changing a number of computers executing intrusion detection software based on time of day, not based on network congestion. The Yavatkar/Porras combination fails teach or suggest all the features of claim 26 and thus fails to establish a *prima facie* case of obviousness. For at least this reason, claim 26 is properly allowable.

Claim 37 recites, in part, a stop condition that is an expiration time. The Yavatkar/Porras combination does not teach such a stop condition, and a *prima facie* case of obviousness has not been established. In addition, the Office action contends that "it is well known to one of ordinary skill in the art that network entities can be scheduled to dynamically instantiate start, suspend, stop, and destroy services," citing Yavatkar, page 161. The Office action admits that Yavatkar does not explicitly teach an expiration time. Office action at page 10. As noted above, the cited portions of Porras do not teach an expiration time either. Thus, the Yavatkar/Porras

combination fails to teach all the features of claim 37, and a *prima facie* case of obviousness has not been established. For at least this reason, claim 37 is properly allowable.

New Claims

New dependent claims 39-43 recite additional features that are not taught or suggested by the Yavatkar/Porras combination. These claims are properly allowable in view of the allowability of their base claim.

Conclusion

In view of the preceding amendments and remarks, all pending claims are in condition for allowance and action to such end is requested. Applicant requests a telephonic interview prior to receiving an Office action responsive to this Amendment to reach a common understanding of Yavatkar. It is believed that such an understanding would advance the prosecution of this application.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 595-5301

By _____
Michael D. Jones
Registration No. 41,879